

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, Jonathan Joyce, being duly sworn, deposes and says that I am a Special Agent with the Federal Bureau of Investigation (“FBI”), duly appointed according to law and acting as such.

Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 1956(h), Conspiracy to Commit Money Laundering, have been committed by LIN KAI, and others, known and unknown.

The source of your affiant’s information and the grounds for his belief are as follows:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation, an investigative and law enforcement officer of the United States, within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure. I have been employed by the Federal Bureau of Investigation (“FBI”) since January 2015 as a Special Agent. I am currently assigned to the FBI Cleveland Division White Collar Squad, which is responsible for investigations involving frauds and swindles to include mail/wire fraud, complex investigations that included securities fraud, insider trading and money laundering cases. I have received specialized training at the FBI Academy, in Quantico, Virginia, in a variety of Federal criminal violations, including training on how to conduct surveillance, electronic and physical searches, interview and interrogation techniques, financial investigations (including asset forfeiture and money laundering tactics), evidence collection, responding to and investigating weapons of mass destruction, arrest and search warrant executions, and case preparation. Prior to joining the FBI, I was a State Certified peace officer in the State of Illinois for approximately eight and a half years. While a police officer, in the City of Oakbrook Terrace, Illinois for over six years I was assigned to the patrol

division. I later became a police officer in the Village of Downers Grove, Illinois and was assigned to the patrol division and investigations. While assigned to investigations I was assigned to the tactical unit and investigated cases that involved vice crimes such as human trafficking, prostitution, and drug crimes. While in the FBI, I have investigated various financial crimes, analyzed pen register and telephone toll data, conducted open-source social media research, analyzed financial records, participated in witness and subject interviews, and participated in the execution of warrants to include the search and seizure of electronic communications accounts, to include emails, social media accounts, messaging applications, and other electronically stored information.

2. I have personally participated in the investigation of LIN KAI, among others, as discussed below. I am familiar with the facts and circumstances of this investigation, through discussions with other law enforcement agents involved in this investigation.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. Victim-1 is 68-year-old resident of Holmesville, Ohio.

5. Starting in late August or early September 2023, Victim-1 started to receive communication requests from an unknown individual using the name CAITRONIA LEE (“LEE”) over Facebook. Victim-1 responded to the Facebook request and LEE began messaging with Victim-1 about Victim-1’s interest in hunting.

6. Victim-1 communicated with LEE over Facebook messenger and discussed his desire to hunt wild animals in Africa. In message conversation with Victim-1, LEE offered Victim-1 an investment opportunity to make a significant amount of money so he could eventually travel to Africa and hunt wild animals. Additionally, LEE offered to be an investment partner with Victim-1.

7. LEE continued the discussion with Victim-1 about the investment opportunity and requested Victim-1 to communicate using an encrypted phone application called WhatsApp. LEE communicated with Victim-1 from the WhatsApp phone number (415) 906-1511.

8. At the direction of LEE, Victim-1 downloaded a crypto currency phone application from the application store on Victim-1's phone. The application on Victim-1's phone appeared as an application for "crypto.com." The affiant reviewed screenshots of the downloaded phone application on Victim-1's phone. The affiant observed another screenshot while inside the "crypto.com" application and saw that the application was not in fact crypto.com, but instead displayed the name Indoda-x.

9. It is the affiant's knowledge and experience in these fraudulent schemes, that bad actors will create similar email addresses, names, websites, and downloadable phone applications to give the appearance to a potential victim that they are accessing the actual website, business, or cryptocurrency exchange website or interface for their investment. Furthermore, the fraudulent website or interface appears to mirror the legitimate website or business, however, the money the victim eventually invests is not going to the actual company, but fraudulently going to the bad actors causing the victim to lose their money. The bad actors have control of the website or phone application and have the ability to reflect the victim's investment and fraudulently inflate the balance of the account to further influence the victim to invest more money. The

company, Indodax, is a legitimate cryptocurrency exchange located in Indonesia, however, a review of the screenshots of Victim-1's phone reveal that the downloaded phone application is Indoda-x.

10. Upon downloading the crypto currency application, Victim-1 was directed with the assistance of LEE to deposit United States legal tender with the utilization of a "service director" that worked at the crypto currency application business. Victim-1 began to communicate with the WhatsApp number (213) 682-9495 related to conducting several United States currency deposits.

11. LEE also provided Victim-1 a hyperlink for access to the account via WhatsApp.

12. On or about September 21, 2023, Victim-1 sent a WhatsApp communication to the service director asking if there were offline transactions support in the United States. The service director responded that the platform would accept "face-to-face cash transactions." Victim-1 further requested if the face-to-face cash transactions could be completed in the State of Ohio. The service director responded that a cash transaction could take place, however, an appointment would need to be made "1-2 working days in advance."

13. On or about September 25, 2023, Victim-1 sent a WhatsApp message to the service director stating Victim-1's desire to buy cryptocurrency by setting up an appointment with a merchant to conduct a face-to-face transaction with the deposit of \$100,000. The service director responded and requested Victim-1's address and phone number. Victim-1 provided an address of Lowe's, 1010 Coshocton Avenue, Mt. Vernon, Ohio, and his personal phone number. Victim-1 also requested additional information concerning the cash face-to-face deposits.

14. The service director responded that upon Victim-1 handing over the cash deposit of \$100,000 during the face-to-face meeting with the merchant, the merchant would contact the

platform to inform them that Victim-1's cash deposit was handed over. The service director explained that the merchant would stay with Victim-1 until the deposit was reflected in Victim-1's digital phone application.

15. The service director then provided a phone number of the merchant that would meet with Victim-1 for the face-to-face cash deposit. The number the service director provided was the WhatsApp number (929) 426-7289. The service director also provided the picture of a United States one-dollar bill with the serial number F36646005G and explained that the merchant will come to the face-to-face meeting with this exact one-dollar bill. The service director instructed Victim-1 to write the date and amount of the deposit on the dollar bill during the cash deposit.

16. On or about September 27, 2023, Victim-1 parked in the parking lot of a Lowe's, 1010 Coshocton Avenue, Mt. Vernon, Ohio. Victim-1 stated an individual approached Victim-1's vehicle and Victim-1 provided the individual \$100,000. Victim-1 was provided a United States one-dollar bill matching the serial number F36646005G. Victim-1 wrote the date and amount of the cash deposit of \$100,000 and sent the picture to the service director.

17. During the face-to-face cash deposit, Victim-1 was also sending LEE WhatsApp messages to confirm the deposit of \$100,000 with the service director and merchant were continuing as planned. Victim-1 reviewed the downloaded crypto currency application on his phone and the deposit of \$100,000 appeared in the account of Victim-1. The merchant then walked away and left the parking lot in a vehicle.

18. On or about October 17, 2023, Victim-1 contacted the service director to conduct an additional deposit of \$277,000 in a face-to-face cash deposit with a merchant. The service director asked Victim-1 if he was satisfied with the \$100,000 deposit that occurred on September

27, 2023. Victim-1 responded to the service director about being satisfied and stated he, Victim-1, wanted to deposit an additional \$277,000 in \$100 United States bills.

19. The service director responded to Victim-1 that the platform would be looking for a merchant to conduct the face-to-face cash deposit. Victim-1 asked the service director if the service director would send the picture of a one-dollar bill again similar to the last transaction. The service direction responded “Yes, this is a safe transaction” and to “Please confirm your purchase amount is 277K.” Victim-1 confirmed the deposit would be “277K.” Approximately two hours later, the service director responded to Victim-1 and provided the phone number 516-585-1693 and provided the picture of a United States one-dollar bill with the serial number D13410439D.

20. On or about October 19, 2023, Victim-1 parked in the parking lot of Lowe’s, 1010 Coshocton Avenue, Mt. Vernon, Ohio. Victim-1 stated an individual approached Victim-1’s vehicle and Victim-1 provided the individual \$277,000. Victim-1 was provided a United States one-dollar bill matching the serial number D134104039D, and Victim-1 wrote the date and amount of the cash deposit of \$277,000 on the one-dollar bill.

21. During the face-to-face cash deposit, Victim-1 was also sending LEE WhatsApp messages to confirm the deposit of \$277,000 with the service director and merchant were continuing as planned. Victim-1 confirmed with the service director the cash payment had been made with the merchant. The service director informed Victim-1 the \$277,000 was being “injected” into the account. Victim-1 reviewed the downloaded crypto currency application on his phone and the deposit of \$277,000 appeared in the account of Victim-1. The merchant then walked away and left the parking lot in a vehicle.

22. On or about November 3, 2023, Victim-1 sent a WhatsApp message to the service director requesting a deposit of \$240,000. The service director confirmed the deposit and provided the merchant phone number (929) 410-0826. The service director also provided the picture of a United States one-dollar bill serial number D03773721D. Victim-1 requested the face-to-face cash deposit location at 1010 Coshocton Ave, Mt. Vernon, Ohio. The service director responded that the merchant would contact Victim-1 and confirm the location and time of the face-to-face deposit.

23. On or about November 4, 2023, Victim-1 parked in the parking lot of Lowe's, 1010 Coshocton Avenue, Mt. Vernon, Ohio. Victim-1 stated an individual approached Victim-1's vehicle and Victim-1 provided the individual \$240,000. Victim-1 was provided a United States one-dollar bill matching the serial number D03773721D. Victim-1 wrote the incorrect date of October 4, 2023, and \$240,000 on the dollar bill.

24. During the face-to-face cash deposit, Victim-1 was also sending LEE WhatsApp messages to confirm the deposit of \$240,000. Victim-1 confirmed with the service director the cash payment was being completed. Victim-1 verified the deposit had been added to the downloaded crypto currency application on his phone and the \$240,000 appeared in the account of Victim-1. The merchant then walked away and left the parking lot in a vehicle.

25. On or about November 17, 2023, Victim-1 contacted the service director and requested a face-to-face deposit of \$400,000. The service director responded, "Please wait, merchants are being matched for you." The service director responded approximately 18 minutes later and provided the merchant phone number (646) 286-9140. The service director also provided the image of a United States one dollar bill with the serial number G71319835A. The service director then questioned Victim-1 who answered the phone call with the merchant to

confirm the face-to-face transaction believing that Victim-1 was a woman. Victim-1 confirmed he was the one who answered the phone call with the merchant and stated he was not a woman.

26. The merchant recontacted Victim-1 to confirm the appropriate location, time and place for the face-to-face transaction and deposit. Victim-1 contacted the merchant and confirmed the date and time being the following day of November 18, 2023.

27. On or about November 18, 2023, Victim-1 parked in the parking lot of Lowe's 1010 Coshocton, Mt. Vernon, Ohio. Victim-1 stated an individual exited a vehicle and approached his vehicle. Victim-1 provided the individual that approached his vehicle \$400,000. Victim-1 was provided a United States one-dollar bill matching the serial number G71319835A. Victim-1 wrote the date of November 18, 2023, and the deposit amount \$400,000. Victim-1 provided the picture to the service director.

28. During the face-to-face cash deposit, Victim-1 was also sending LEE WhatsApp messages to confirm the deposit of \$400,000. Victim-1 confirmed with the service director that the cash payment was being completed. Victim-1 verified the deposit had been added to the downloaded crypto currency application on his phone and the \$400,000 appeared in the account of Victim-1. The merchant then walked away and left the parking lot in a vehicle.

29. On or about December 5, 2023, Victim-1 contacted the service director and requested a face-to-face deposit of \$300,000. The service director responded to Victim-1 to wait while a merchant was identified to assist with the face-to-face transaction. The service director responded approximately 51 minutes later and provided the merchant phone number (929) 679-0809. The service director also provided the image of a United States one-dollar bill with the serial number D10924511D.

30. On or about December 7, 2023, Victim-1 parked in the parking lot of Lowe's, 1010 Coshocton Avenue, Mt. Vernon, Ohio. Victim-1 stated an individual exited a vehicle and approached his vehicle. Victim-1 provided the individual that approached his vehicle \$300,000. Victim-1 was provided a United States one-dollar bill matching the serial number D10924511D. Victim-1 wrote the date of Dec. 7, 2023, and the deposit amount \$300,000. Victim-1 provided the picture to the service director.

31. During the face-to-face cash deposit, Victim-1 was also sending LEE WhatsApp messages to confirm the deposit of \$300,000. Victim-1 confirmed with the service director that cash payment was being completed. The merchant received the \$300,000 and left the parking lot in a vehicle. The service director told Victim-1 the transaction was successful.

32. Over the course of depositing cash with the service director, Victim-1 continued to observe his investment grow. Victim-1, upon reaching a balance of approximately \$15,000,00, decided to withdraw the funds due to the accumulated investment amount. Victim-1 requested the withdrawal of the investment to be sent to his financial institution located in the United States. Victim-1 connected his personal banking account to the crypto currency phone application to receive funds in the form of a withdrawal.

33. When the funds were not sent to his financial institution as requested, Victim-1 became concerned and contacted the service director.

34. On or about December 8, 2023, Victim-1 messaged the service director regarding his unsuccessful attempts to withdrawal from his crypto account. Victim-1 sent a screenshot of the account to the service director confirming the amount of his investment was now \$15,180,500.80. The service director requested the account number from Victim-1 and directed

Victim-1 where to find the account number on the downloaded crypto currency phone application.

35. Victim-1 identified the account number and provided a screenshot to the service director. The service director responded to Victim-1 stating “Your withdrawal did not pass the review of the blockchain center and was carried out using a large amount of mixed funds. Investment, triggering the anti-money laundering risk control system and your cryptocurrency cannot be transferred.”

36. The service director required Victim-1 to provide transfer information related to LEE’s purported \$2.4 million investment that was invested from China into the downloaded crypto currency account created by Victim-1. Victim-1 responded to the service director stating the LEE’s \$2.4 million purported investment was from a mortgage company and additional documentation sounding the investment could not be provided. Without being able to provide additional documentation about the \$2.4 million investment, Victim-1 requested additional assistance from the service director in order to withdrawn his total investment. The service director responded, “you can only remove the account risk control problem through the capital verification process.”

37. Victim-1 asked the service director if he added an additional \$2.4 million into the account within the next few days would all the funds be transferred into his financial institution account based in the United States. The service director confirmed that by adding an additional \$2.4 million into the account, Victim-1 would receive the refund from the investment.

38. Realizing that he may be the victim of a scam, on or about December 18, 2023, Victim-1 filed a police report with the Holmes County Sheriff’s Office. Victim-1 related to the Holmes County Sheriff’s Office that, at times, communications over WhatsApp and on Facebook

with LEE occurred while at his address in Holmes County. The request for Victim-1 to join into the cryptocurrency investment platform occurred in Holmes County. Holmes County Sheriff's Office took photographs of the communications with Victim-1 and the service director as part of their initial investigation.

39. Victim-1 is currently in contact with LEE and the service director concerning the \$2.4 million required to transfer the investment from Victim-1's account.

40. On or about January 5, 2024, at the direction of the FBI, Victim-1 sent a WhatsApp text message to LEE about depositing an additional \$120,000 to fix the issue with the account with the remaining amount needed being deposited before the account would be frozen.

41. FBI obtained \$120,000 in controlled funds with the intent to conduct a controlled delivery of the funds to the purported merchant for the cryptocurrency phone application.

42. On January 9, 2024, Victim-1 contacted the service director requesting a deposit of \$120,000 with a face-to-face deposit with a merchant.

43. On January 10, 2024, Victim-1 contacted the service director requesting a deposit of \$120,000 with a domestic wire instruction per the request of the service director. The service director provided the instructions to wire the \$120,000 to an account in the name of 385 Trading Inc. Victim-1 shortly thereafter responded to the service director and provided a letter from the financial institution that stated Victim-1 had attempted the wire deposit and stated the \$120,000 could not be wired to the account of 385 Trading Inc. due to potential red flags and fraudulent activity.

44. Victim-1 asked the service director if there was a merchant available for a face-to-face deposit of funds in the amount of \$120,000. The service director confirmed there was a

merchant available however he required more than \$300,000 to conduct a face-to-face deposit of funds.

45. On January 18, 2024, the FBI obtained approximately \$1,250,000 in counterfeit funds with the intent to conduct a controlled delivery of the funds to the purported merchant for the cryptocurrency phone application.

46. Victim-1 sent photographs of the FBI obtained counterfeit funds along with the \$120,000 controlled funds to the service director and requested a face-to-face deposit with a merchant in the amount of \$1,500,000. The service director responded to Victim-1 asking if the face-to-face deposit would occur at the same location as before. The service director initially requested the face-to-face deposit to be split due to the large amount being deposited.

47. The service director responded to Victim-1 and stated via text message that there would be a one-time transaction for \$1,400,000 and the service director would provide the merchant's phone number. The service director then provided the phone number of +1 929-726-0728. The service director also provided the image of a United States one-dollar bill with the serial number G75297833E.

FBI OPERATION ON JANUARY 20, 2024

48. On January 20, 2024, Victim-1 drove to the Lowe's, 1010 Coshocton, Mount Vernon, Ohio and parked in the parking lot with the cash.

49. FBI agents and local law enforcement conducted surveillance around the Lowe's and in the Mt. Vernon area. FBI agents observed a dark colored Toyota Highlander XLE AWD bearing New York registration KWW3331, ("SUBJECT VEHICLE 1") driven by an asian male individual later identified as LIN KAI ("KAI"), enter the Lowe's parking lot and park next to Victim-1. KAI exited the driver seat of the Toyota and entered the passenger front seat of

Victim-1's vehicle. Law enforcement recorded the conversation with Victim-1 and KAI. Victim-1 was provided the United States single-dollar bill with serial G75297833E. Victim-1 wrote the date and \$1.4 million on the United States single-dollar bill and took a photograph of it. Victim-1 sent a picture of the United States single-dollar bill and provided it to the service director. Victim-1 then reviewed his cryptocurrency phone application and observed the deposit reflected into his account. KAI took pictures of the FBI controlled funds and upon the completed transaction in Victim-1's account, KAI exited the Victim-1's vehicle.

50. KAI reapproached his vehicle and opened the rear drive side door and placed the bag of \$1,400,000 of FBI controlled funds into the vehicle. KAI was then approached by law enforcement officers and placed into custody.

51. KAI was searched and an Apple I-phone, two sim cards, and a driver's license were located on KAI's person.

52. KAI was transported to the Knox County Sheriff's Office.

53. During a search of SUBJECT VEHICLE 1, FBI agents recovered the \$1,400,000 of controlled FBI funds and tracking device from SUBJECT VEHICLE 1.

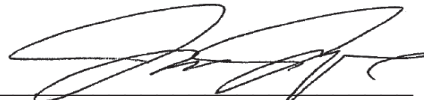
54. While KAI was in custody, he was interviewed and told FBI agents that he was directed by another individual to pick up a package from Victim-1. KAI was picking up a package for the other individual's business, however, did not know what the other individual did as a business. KAI would be given a cellular phone in his mailbox and would be provided instructions to pick up a package from Victim-1. KAI had picked up money from Victim-1 three times, and each time the package contained money. KAI had never picked up anything other than money from Victim-1. KAI was instructed by another individual upon receiving the

package from Victim-1, he was to destroy the sim card in the Apple I-phone and to replace it with one from his pocket.

55. KAI, after replacing the sim card and after receiving the package, was instructed to drive for the next 30 minutes to an hour and then exit the road and to call the other individual. The other individual would arrange for another person to pick up the package from KAI. KAI stated he received \$2,000 for picking up each package from Victim-1.

CONCLUSION

56. Based on the totality of the facts and circumstances set forth herein, and based upon my training and experience, there is probable cause to believe, and I do believe LIN KAI engaged in conspiracy to commit money laundering, in violation of Title 18, United States Code, Section 1956(h). Accordingly, I respectfully request that the Court issue a Federal Criminal Complaint authorizing the arrest of LIN KAI.



Special Agent Jonathan Joyce
Federal Bureau of Investigation

Sworn to via telephone on January 22nd, 2024, after submission by reliable electronic means.
Fed. R. Crim. P. 3, 4(d), and 4.1.


Amanda M. Knapp
United States Magistrate Judge